

# SOME REE AND SUZUKI CURVES ARE NOT GALOIS COVERED BY THE HERMITIAN CURVE

MARIA MONTANUCCI AND GIOVANNI ZINI

**ABSTRACT.** The Deligne-Lusztig curves associated to the algebraic groups of type  ${}^2A_2$ ,  ${}^2B_2$ , and  ${}^2G_2$  are classical examples of maximal curves over finite fields. The Hermitian curve  $\mathcal{H}_q$  is maximal over  $\mathbb{F}_{q^2}$ , for any prime power  $q$ , the Suzuki curve  $\mathcal{S}_q$  is maximal over  $\mathbb{F}_{q^4}$ , for  $q = 2^{2h+1}$ ,  $h \geq 1$  and the Ree curve  $\mathcal{R}_q$  is maximal over  $\mathbb{F}_{q^6}$ , for  $q = 3^{2h+1}$ ,  $h \geq 0$ . In this paper we show that  $\mathcal{S}_8$  is not Galois covered by  $\mathcal{H}_{64}$ . We also give a proof for an unpublished result due to Rains and Zieve stating that  $\mathcal{R}_3$  is not Galois covered by  $\mathcal{H}_{27}$ . Furthermore, we determine the spectrum of genera of Galois subcovers of  $\mathcal{H}_{27}$ , and we point out that some Galois subcovers of  $\mathcal{R}_3$  are not Galois subcovers of  $\mathcal{H}_{27}$ .

## 1. INTRODUCTION

Let  $q$  be a prime power,  $\mathbb{F}_{q^2}$  be the finite field with  $q^2$  elements, and  $\mathcal{X}$  be an  $\mathbb{F}_{q^2}$ -rational curve, i.e. a projective, absolutely irreducible, non-singular algebraic curve defined over  $\mathbb{F}_{q^2}$ . The curve  $\mathcal{X}$  is called  $\mathbb{F}_{q^2}$ -maximal if the number  $|\mathcal{X}(\mathbb{F}_{q^2})|$  of its  $\mathbb{F}_{q^2}$ -rational points attains the Hasse-Weil upper bound

$$q^2 + 1 + 2gq,$$

where  $g$  is the genus of  $\mathcal{X}$ . Maximal curves have interesting properties and have also been investigated for their applications in Coding Theory. Surveys on maximal curves are found in [8, 9, 10, 12, 40, 41] and [23, Chapt. 10].

By a result commonly attributed to Serre, see [28, Prop. 6], any  $\mathbb{F}_{q^2}$ -rational curve which is  $\mathbb{F}_{q^2}$ -covered by an  $\mathbb{F}_{q^2}$ -maximal curve is also  $\mathbb{F}_{q^2}$ -maximal. In particular,  $\mathbb{F}_{q^2}$ -maximal curves can be obtained as Galois  $\mathbb{F}_{q^2}$ -subcovers of an  $\mathbb{F}_{q^2}$ -maximal curve  $\mathcal{X}$ , that is as quotient curves  $\mathcal{X}/G$  for a finite  $\mathbb{F}_{q^2}$ -automorphism group  $G \leq \text{Aut}(\mathcal{X})$ . Most of the known maximal curves are Galois subcovers of one of the Deligne-Lusztig curves; see e.g. [14, 5, 15] for subcovers of the Hermitian curve  $\mathcal{H}_q : X^{q+1} + Y^{q+1} + T^{q+1} = 0$ , [17, 32] for subcovers of the Suzuki curve  $\mathcal{S}_q : Y^q + Y = X^{q_0}(X^q + X)$ , with  $q = 2q_0^2$ ,  $q_0 = 2^h$ ,  $h \geq 0$ , [2, 3, 33] for subcovers of the Ree curve  $\mathcal{R}_q : Y^q - Y = X^{q_0}(X^q - X)$ ,  $Z^q - Z = X^{q_0}(Y^q - Y)$ , with  $q = 3q_0^2$ ,  $q_0 = 3^h$ ,  $h \geq 0$ , and the references therein.

The first example of a maximal curve not Galois covered by the Hermitian curve was discovered by Garcia and Stichtenoth [13]. This curve is  $\mathbb{F}_{36}$ -maximal and not Galois covered by  $\mathcal{H}_{27}$ . It is a special case of the  $\mathbb{F}_{q^6}$ -maximal GS curve, which was recently shown not to be Galois covered by  $\mathcal{H}_{q^3}$  for any  $q > 3$  [18, 29]. Giulietti and Korchmáros

[16] provided an  $\mathbb{F}_{q^6}$ -maximal curve, nowadays referred to as the GK curve, which is not covered by the Hermitian curve  $\mathcal{H}_{q^3}$  for any  $q > 2$ . In [38, 19], some subcovers of the GK curve were shown not to be covered, or Galois covered, by the Hermitian curve. Garcia, Güneri, and Stichtenoth [11] generalized the GK curve to an  $\mathbb{F}_{q^{2n}}$ -maximal curve, for any  $q$  and any odd  $n \geq 3$ . The generalized GK curve is not Galois covered by  $\mathcal{H}_{q^n}$  for any  $n \geq 5$ , as shown in [7] for  $q > 2$  and in [18] for  $q = 2$ .

It is a challenging task to decide whether a DL-curve of Ree or Suzuki type is a Galois subcover of the Hermitian curve. In this paper we prove the following results.

**Theorem 1.1.** *The Suzuki curve  $\mathcal{S}_8$  is not Galois covered by the Hermitian curve  $\mathcal{H}_{64}$ .*

**Theorem 1.2.** *The Ree curve  $\mathcal{R}_3$  is not Galois covered by the Hermitian curve  $\mathcal{H}_{27}$ .*

**Proposition 1.3.** *The Suzuki curve  $\mathcal{S}_2$  is Galois covered by the Hermitian curve  $\mathcal{H}_4$ .*

We note that Theorem 1.2 is an unpublished result due to Rains and Zieve.

We give an outline of the proofs of Theorems 1.1 and 1.2. We first bound the possible degrees  $d$  of putative Galois coverings  $\mathcal{H}_{64} \rightarrow \mathcal{S}_8$  and  $\mathcal{H}_{27} \rightarrow \mathcal{R}_3$  from the Riemann-Hurwitz formula; see [37, Theorem 3.4.13]. Then, for each possible value of  $d$ , we investigate all subgroups  $G$  of  $\text{PGU}(3, 64)$  and  $\text{PGU}(3, 27)$  having order  $d$ . The structure of  $G$  allows us to estimate the contribution to the degree  $\Delta$  of the different divisor for each element of  $G$ ; see [37, Theorem 3.8.7]. In most cases, we get that the genus of the quotient curve is different from that of  $\mathcal{S}_8$  and  $\mathcal{R}_3$ . Sometimes, a deeper investigation of the automorphism group of the quotient curve  $\mathcal{H}_{64}/G$  or  $\mathcal{H}_{27}/G$  is needed. As a by-product, we describe in Proposition 3.1 the unique quotient curve  $\mathcal{X}$  of  $\mathcal{H}_{64}$  which has the same genus as  $\mathcal{S}_8$ ;  $\mathcal{X}$  is defined over  $\mathbb{F}_8$ . Since  $\mathcal{X}$  is not isomorphic to  $\mathcal{S}_8$ , a result by Fuhrmann and Torres [8, Theorem 5.1] implies that  $\mathcal{X}$  is not  $\mathbb{F}_8$ -optimal. We also describe in Proposition 4.1 the quotient curves of  $\mathcal{H}_{27}$  which have the same genus of  $\mathcal{R}_3$ . More generally, we determine in Theorem 5.1 the spectrum of genera of Galois subcovers of  $\mathcal{H}_{27}$ . For all  $g > 1$ , we classify all subgroups  $G \leq \text{PGU}(3, 27)$  such that the quotient curve  $\mathcal{H}_{27}/G$  has genus  $g$ . We point out that some quotient curves of  $\mathcal{R}_3$ , studied by Çakçak and Özbudak [2], are not quotient curves of  $\mathcal{H}_{27}$ ; see Corollary 5.2.

Results by Garcia, Stichtenoth, and Xing [14] on the automorphism groups of the Hermitian curve  $\mathcal{H}_q$  fixing an  $\mathbb{F}_{q^2}$ -rational point of  $\mathcal{H}_q$  will be used. We also rely on classical classification results of subgroups of  $\text{PSU}(3, q)$  by Mitchell [30] and Hartley [22].

We classify the elements of  $\text{PGU}(3, q)$  in terms of their orders and their action on  $\text{PG}(2, \overline{\mathbb{F}}_q)$  and  $\mathcal{H}_q$ . In this way, we get the contribution to  $\Delta$  of any element of  $\text{PGU}(3, q)$ , in terms of its geometric properties; see Theorem 2.7. This is a result of independent interest, which extends [7, Lemma 4.1].

The paper is organized as follows. In Section 2 we present the preliminary results on quotient curves of the Hermitian curve and the proof of Proposition 1.3. Sections 3 and 4

contain the proofs of Theorems 1.1 and 1.2, respectively. Section 5 provides the spectrum of genera of quotient curves of  $\mathcal{H}_{27}$  and three examples of quotient curves of  $\mathcal{R}_3$  which are not quotient curves of  $\mathcal{H}_{27}$ .

## 2. PRELIMINARY RESULTS

Throughout this paper,  $q = p^n$ , where  $p$  is a prime number and  $n$  is a positive integer. The Deligne-Lusztig curves defined over a finite field  $\mathbb{F}_q$  were originally introduced in [6]. Other than the projective line, there are three families of Deligne-Lusztig curves, named Hermitian curves, Suzuki curves and Ree curves. These curves are maximal over some finite field containing  $\mathbb{F}_q$ . The following descriptions with explicit equations come from [20, 21].

- The Hermitian curve  $\mathcal{H}_q$  arises from the algebraic group  ${}^2A_2(q) = \text{PGU}(3, q)$  of order  $(q^3 + 1)q^3(q^2 - 1)$ . It has genus  $q(q - 1)/2$  and is  $\mathbb{F}_{q^2}$ -maximal. Two ( $\mathbb{F}_{q^2}$ -projectively equivalent) nonsingular plane models of  $\mathcal{H}_q$  are the Fermat curve with homogeneous equation

$$(2.1) \quad X^{q+1} + Y^{q+1} + T^{q+1} = 0$$

and the norm-trace curve with homogeneous equation

$$(2.2) \quad Y^{q+1} = X^q T + X T^q.$$

The automorphism group  $\text{Aut}(\mathcal{H}_q)$  is isomorphic to the projective unitary group  $\text{PGU}(3, q)$ , and it acts on the set  $\mathcal{H}_q(\mathbb{F}_{q^2})$  of all  $\mathbb{F}_{q^2}$ -rational points of  $\mathcal{H}_q$  as  $\text{PGU}(3, q)$  in its usual 2-transitive permutation representation.

- The Suzuki curve  $\mathcal{S}_q$  arises from the simple Suzuki group  ${}^2B_2(q) = Sz(q)$ . It has genus  $q_0(q - 1)$  and is  $\mathbb{F}_{q^4}$ -maximal, where  $q = 2q_0^2$ ,  $q_0 = 2^h$ ,  $h \geq 1$ . A (singular) plane model of  $\mathcal{S}_q$  is given by the affine equation

$$Y^q + Y = X^{q_0}(X^q + X).$$

The automorphism group  $\text{Aut}(\mathcal{S}_q)$  is isomorphic to a subgroup of the projective group  $\text{PGL}(4, q)$  preserving the Suzuki-Tits ovoid  $O_S$  in  $\text{PG}(3, q)$ , and it acts on  $O_S$  as  $Sz(q)$  in its usual 2-transitive permutation representation.

- The Ree curve  $\mathcal{R}_q$  arises from the simple Ree group  ${}^2G_2(q) = \text{Ree}(q)$ . It has genus  $3q_0(q - 1)(q + q_0 + 1)/2$  and is  $\mathbb{F}_{q^6}$ -maximal, where  $q = 3q_0^2$ ,  $q_0 = 3^h$ ,  $h \geq 0$ . A (singular) space model of  $\mathcal{R}_q$  is given by the affine equations

$$Y^q - Y = X^{q_0}(X^q - X), \quad Z^q - Z = X^{q_0}(Y^q - Y).$$

The automorphism group  $\text{Aut}(\mathcal{R}_q)$  is isomorphic to a subgroup of the projective group  $\text{PGL}(7, q)$  preserving the Ree-Tits ovoid  $O_R$  in  $\text{PG}(6, q)$ , and it acts on  $O_R$  as  $\text{Ree}(q)$  in its usual 2-transitive permutation representation.

We extend the definition of a Suzuki curve to the case  $q = 2$ . A (singular) plane model of  $\mathcal{S}_2$  is given by the

$$\mathcal{S}_2 : Y^2 + Y = X(X^2 + X).$$

In particular,  $\mathcal{S}_2$  is an elliptic and  $\mathbb{F}_{2^4}$ -maximal curve.

The combinatorial properties of  $\mathcal{H}_q(\mathbb{F}_{q^2})$  can be found in [25]. The size of  $\mathcal{H}_q(\mathbb{F}_{q^2})$  is equal to  $q^3 + 1$ , and a line of  $PG(2, q^2)$  has either 1 or  $q + 1$  common points with  $\mathcal{H}_q(\mathbb{F}_{q^2})$ , that is, it is either a 1-secant or a chord of  $\mathcal{H}_q(\mathbb{F}_{q^2})$ . Furthermore, a unitary polarity is associated with  $\mathcal{H}_q(\mathbb{F}_{q^2})$  whose isotropic points are those of  $\mathcal{H}_q(\mathbb{F}_{q^2})$  and isotropic lines are the 1-secants of  $\mathcal{H}_q(\mathbb{F}_{q^2})$ , that is, the tangents to  $\mathcal{H}_q$  at the points of  $\mathcal{H}_q(\mathbb{F}_{q^2})$ .

From Group theory we need the classification of all maximal subgroups of the projective special subgroup  $PSU(3, q)$  of  $PGU(3, q)$ , going back to Mitchell and Hartley; see [30], [22], [24].

**Theorem 2.1.** *Let  $d = \gcd(3, q+1)$ . Up to conjugacy, the subgroups below give a complete list of maximal subgroups of  $PSU(3, q)$ .*

- (i) *the stabilizer of an  $\mathbb{F}_{q^2}$ -rational point of  $\mathcal{H}_q$ . It has order  $q^3(q^2 - 1)/d$ ;*
- (ii) *the stabilizer of an  $\mathbb{F}_{q^2}$ -rational point off  $\mathcal{H}_q$  (equivalently the stabilizer of a chord of  $\mathcal{H}_q(\mathbb{F}_{q^2})$ ). It has order  $q(q - 1)(q + 1)^2/d$ ;*
- (iii) *the stabilizer of a self-polar triangle with respect to the unitary polarity associated to  $\mathcal{H}_q(\mathbb{F}_{q^2})$ . It has order  $6(q + 1)^2/d$ ;*
- (iv) *the normalizer of a (cyclic) Singer subgroup. It has order  $3(q^2 - q + 1)/d$  and preserves a triangle in  $PG(2, q^6) \setminus PG(2, q^2)$  left invariant by the Frobenius collineation  $\Phi_{q^2} : (X, Y, T) \mapsto (X^{q^2}, Y^{q^2}, T^{q^2})$  of  $PG(2, \mathbb{F}_q)$ ;*  
for  $p > 2$ :
  - (v)  $PGL(2, q)$  preserving a conic;
  - (vi)  $PSU(3, p^m)$  with  $m \mid n$  and  $n/m$  odd;
  - (vii) subgroups containing  $PSU(3, p^m)$  as a normal subgroup of index 3, when  $m \mid n$ ,  $n/m$  is odd, and 3 divides both  $n/m$  and  $q + 1$ ;
  - (viii) the Hessian groups of order 216 when  $9 \mid (q + 1)$ , and of order 72 and 36 when  $3 \mid (q + 1)$ ;
  - (ix)  $PSL(2, 7)$  when  $p = 7$  or  $-7$  is not a square in  $\mathbb{F}_q$ ;
  - (x) the alternating group  $Alt(6)$  when either  $p = 3$  and  $n$  is even, or 5 is a square in  $\mathbb{F}_q$  but  $\mathbb{F}_q$  contains no cube root of unity;
  - (xi) the symmetric group  $Sym(6)$  when  $p = 5$  and  $n$  is odd;
  - (xii) the alternating group  $Alt(7)$  when  $p = 5$  and  $n$  is odd;
- for  $p = 2$ :
  - (xiii)  $PSU(3, 2^m)$  with  $m \mid n$  and  $n/m$  an odd prime;
  - (xiv) subgroups containing  $PSU(3, 2^m)$  as a normal subgroup of index 3, when  $n = 3m$  with  $m$  odd;
  - (xv) a group of order 36 when  $n = 1$ .

In our investigation it is useful to know how an element of  $\text{PGU}(3, q)$  of a given order acts on  $\text{PG}(2, \bar{\mathbb{F}}_q)$ , and in particular on  $\mathcal{H}_q(\mathbb{F}_{q^2})$ . This can be obtained as a corollary of Theorem 2.1, and is stated in Lemma 2.2 with the usual terminology of collineations of projective planes; see [25]. In particular, a linear collineation  $\sigma$  of  $\text{PG}(2, \bar{\mathbb{F}}_q)$  is a  $(P, \ell)$ -perspectivity, if  $\sigma$  preserves each line through the point  $P$  (the *center* of  $\sigma$ ), and fixes each point on the line  $\ell$  (the *axis* of  $\sigma$ ). A  $(P, \ell)$ -perspectivity is either an *elation* or a *homology* according as  $P \in \ell$  or  $P \notin \ell$ . A  $(P, \ell)$ -perspectivity is in  $\text{PGL}(3, q^2)$  if and only if its center and its axis are in  $\text{PG}(2, \mathbb{F}_{q^2})$ .

**Lemma 2.2.** *For a nontrivial element  $\sigma \in \text{PGU}(3, q)$ , one of the following cases holds.*

- (A)  $\text{ord}(\sigma) \mid (q + 1)$ . Moreover,  $\sigma$  is a homology whose center  $P$  is a point off  $\mathcal{H}_q$  and whose axis  $\ell$  is a chord of  $\mathcal{H}_q(\mathbb{F}_{q^2})$  such that  $(P, \ell)$  is a pole-polar pair with respect to the unitary polarity associated to  $\mathcal{H}_q(\mathbb{F}_{q^2})$ .
- (B)  $\text{ord}(\sigma)$  is coprime with  $p$ . Moreover,  $\sigma$  fixes the vertices  $P_1, P_2, P_3$  of a non-degenerate triangle  $T$ .
  - (B1) The points  $P_1, P_2, P_3$  are  $\mathbb{F}_{q^2}$ -rational,  $P_1, P_2, P_3 \notin \mathcal{H}_q$  and the triangle  $T$  is self-polar with respect to the unitary polarity associated to  $\mathcal{H}_q(\mathbb{F}_{q^2})$ . Also,  $\text{ord}(\sigma) \mid (q + 1)$ .
  - (B2) The points  $P_1, P_2, P_3$  are  $\mathbb{F}_{q^2}$ -rational,  $P_1 \notin \mathcal{H}_q$ ,  $P_2, P_3 \in \mathcal{H}_q$ . Also,  $\text{ord}(\sigma) \mid (q^2 - 1)$  and  $\text{ord}(\sigma) \nmid (q + 1)$ .
  - (B3) The points  $P_1, P_2, P_3$  have coordinates in  $\mathbb{F}_{q^6} \setminus \mathbb{F}_{q^2}$ ,  $P_1, P_2, P_3 \in \mathcal{H}_q$ . Also,  $\text{ord}(\sigma) \mid (q^2 - q + 1)$ .
- (C)  $\text{ord}(\sigma) = p$ . Moreover,  $\sigma$  is an elation whose center  $P$  is a point of  $\mathcal{H}_q$  and whose axis  $\ell$  is a tangent of  $\mathcal{H}_q(\mathbb{F}_{q^2})$  such that  $(P, \ell)$  is a pole-polar pair with respect to the unitary polarity associated to  $\mathcal{H}_q(\mathbb{F}_{q^2})$ .
- (D)  $\text{ord}(\sigma) = p$  with  $p \neq 2$ , or  $\text{ord}(\sigma) = 4$  and  $p = 2$ . Moreover,  $\sigma$  fixes an  $\mathbb{F}_{q^2}$ -rational point  $P$ , with  $P \in \mathcal{H}_q$ , and a line  $\ell$  which is a tangent of  $\mathcal{H}_q(\mathbb{F}_{q^2})$ , such that  $(P, \ell)$  is a pole-polar pair with respect to the unitary polarity associated to  $\mathcal{H}_q(\mathbb{F}_{q^2})$ .
- (E)  $p \mid \text{ord}(\sigma)$ ,  $p^2 \nmid \text{ord}(\sigma)$ , and  $\text{ord}(\sigma) \neq p$ . Moreover,  $\sigma$  fixes two  $\mathbb{F}_{q^2}$ -rational points  $P, Q$ , with  $P \in \mathcal{H}_q$ ,  $Q \notin \mathcal{H}_q$ .

*Proof.* Let  $p \mid \text{ord}(\sigma)$ ,  $\text{ord}(\sigma) \neq p$ , and  $(p, \text{ord}(\sigma)) \neq (2, 4)$ . By [30, §2 p. 212] and [22, pp. 141-142], the fixed elements of  $\sigma$  are two points  $P, Q$ , the line  $PQ$ , and another line  $\ell$  through  $P$ . Also,  $p^2 \nmid \text{ord}(\sigma)$ . The Frobenius collineation  $\Phi_{q^2} : (X, Y, T) \mapsto (X^{q^2}, Y^{q^2}, T^{q^2})$  commutes with  $\sigma$ . Hence  $\Phi_{q^2}$  acts on  $\{P, Q\}$ , and  $P, Q$  are  $\mathbb{F}_{q^4}$ -rational. If  $R \in \{P, Q\}$  is the pole of  $PQ$ , then  $R \in \mathcal{H}_q$ . Since  $\mathcal{H}_q$  has no points with coordinates in  $\mathbb{F}_{q^4} \setminus \mathbb{F}_{q^2}$ ,  $R$  is  $\mathbb{F}_{q^2}$ -rational. Thus the line  $PQ$  is a tangent of  $\mathcal{H}_q(\mathbb{F}_{q^2})$  at  $R$ . Hence the pole of  $\ell$  is  $\mathbb{F}_{q^2}$ -rational and off  $\ell$ . Therefore  $R = P$  and the assertions of Case (E) follow.

Let  $\text{ord}(\sigma) = p$ , and let  $\mathcal{H}_q$  have equation (2.2). Up to conjugation,  $\sigma$  is contained in the Sylow  $p$ -subgroup  $S$  of  $\text{PGU}(3, q)$  defined by  $S = \{\tau_{1,b,c} \mid b, c \in \mathbb{F}_{q^2}, b^{q+1} = c^q + c\}$ , where

$$(2.3) \quad \tau_{1,b,c} = \begin{pmatrix} 1 & b^q & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}.$$

Hence  $\sigma$  fixes the  $\mathbb{F}_{q^2}$ -rational point  $P_\infty = (1, 0, 0) \in \mathcal{H}_q$  and its polar line  $\ell_\infty : T = 0$ , which satisfies  $\ell_\infty \cap \mathcal{H}_q = \{P_\infty\}$ . If  $p = 2$ , then  $\sigma$  is of type  $\tau_{1,0,c}$ , and  $\sigma$  is an elation with center  $P_\infty$  and axis  $\ell_\infty$ , which is Case (C). If  $p \neq 2$ , then by [30, §2 p. 212]  $\sigma = \tau_{1,b,c}$  satisfies either Case (C) or Case (D). By direct computation, Cases (C) and (D) correspond to  $b = 0$  and  $b \neq 0$ , respectively.

Let  $p \nmid \text{ord}(\sigma)$ . By [30, §2 p. 212] and [22, pp. 141-142], either  $\sigma$  fixes a point  $P$  and a line  $\ell$  pointwise, or  $\sigma$  fixes exactly three non-collinear points.

Assume that the former case holds. Then  $P$  and  $\ell$  are fixed by  $\Phi_{q^2}$ . Hence, they are defined over  $\mathbb{F}_{q^2}$ . We have  $P \notin \mathcal{H}_q$ . In fact, if  $P \in \mathcal{H}_q$ , then the tangent to  $\mathcal{H}_q$  at  $P$  intersect  $\ell$  at an  $\mathbb{F}_{q^2}$ -rational point  $Q \notin \mathcal{H}_q$ , and the  $\mathbb{F}_{q^2}$ -rational pole  $R$  of  $\ell$  lies on  $\ell$ , hence also on  $\mathcal{H}_q$ . For any  $\mathbb{F}_{q^2}$ -rational point  $\bar{P}$  of  $\ell \setminus \{R\}$ , we have that  $\bar{P} \notin \mathcal{H}_q$  and the polar line of  $\bar{P}$  intersects  $\ell$  at another  $\mathbb{F}_{q^2}$ -rational point of  $\ell$ . Since the line  $PQ$  is the polar line of  $P$ , this is a contradiction. Therefore,  $\ell$  is the polar line of  $P$ , and  $\ell$  is a chord of  $\mathcal{H}_q(\mathbb{F}_{q^2})$ . Now we show that  $\text{ord}(\sigma) \mid (q+1)$ . Let  $\mathcal{H}_q$  have equation (2.1). Up to conjugation,  $P = (0, 0, 1)$  and  $\ell : T = 0$ . Hence  $\sigma$  is a diagonal matrix of the form  $\text{diag}(\lambda, 1, 1)$ , which implies  $\text{ord}(\sigma) = \text{ord}(\lambda)$  with  $\text{ord}(\lambda) \mid (q+1)$ . This shows that  $\sigma$  satisfies Case (A).

Now assume that  $\sigma$  fixes exactly the vertices  $P_1, P_2, P_3$  of a triangle  $T$ .

- Suppose that  $P_1, P_2$ , and  $P_3$  are  $\mathbb{F}_{q^2}$ -rational. If  $P_1, P_2, P_3 \notin \mathcal{H}_q$ , then  $P_j P_k$  is the polar line of  $P_i$ , for  $\{i, j, k\} = \{1, 2, 3\}$ . Let  $\mathcal{H}_q$  have equation (2.1). Up to conjugation  $P_1, P_2$ , and  $P_3$  are the fundamental points. Thus  $\sigma$  is a diagonal matrix and  $\text{ord}(\sigma) \mid (q+1)$ , which is Case (B1). Assume  $P_2 \in \mathcal{H}_q$ . Then the polar line  $\ell_2$  of  $P_2$  is either  $P_1 P_2$  or  $P_2 P_3$ , say  $P_1 P_2$ . The polar line  $\ell_3$  of  $P_3$  is either  $P_1 P_3$  or  $P_2 P_3$ , whence  $P_3 \in \ell_3$  and  $P_3 \in \mathcal{H}_q$ . Then  $\ell_3 \cap \mathcal{H}_q = \{P_3\}$ , and hence  $\ell_3$  is  $P_1 P_3$ . This implies that  $P_2 P_3$  is the polar line of  $P_1$  and  $P_1 \notin \mathcal{H}_q$ . Let  $\mathcal{H}_q$  have equation (2.2). Up to conjugation,  $P_2 = (1, 0, 0)$  and  $P_3 = (0, 0, 1)$ . Thus  $P_1 = (0, 1, 0)$  and  $\sigma$  is the diagonal matrix  $\text{diag}(\mu^{q+1}, \mu, 1)$  for some  $\mu \in \mathbb{F}_{q^2}^*$ . Since  $\sigma$  is not a homology,  $\text{ord}(\sigma) = \text{ord}(\mu)$  does not divide  $q+1$ . This is Case (B2).
- Suppose that  $P_1$  has coordinates in  $\mathbb{F}_{q^6} \setminus \mathbb{F}_{q^2}$ . The orbit of  $P_1$  under  $\Phi_{q^2}$  is  $\{P_1, P_2, P_3\}$ . Hence,  $P_2$  and  $P_3$  have coordinates in  $\mathbb{F}_{q^6} \setminus \mathbb{F}_{q^2}$  as well. Assume  $P_1 \in \mathcal{H}_q$ . Then the polar line  $\ell_1$  of  $P_1$  is tangent to  $\mathcal{H}_q$  at  $P_1$  and  $\ell_1$  has exactly another point  $P$  in common with  $\mathcal{H}_q$ , which is then fixed by  $\sigma$ . Up to reordering,  $P = P_2$ . In the same way,  $P_3 \in \mathcal{H}_q$  and the polar line of  $P_1, P_2, P_3$  are  $P_1 P_2$ ,  $P_2 P_3$ ,  $P_3 P_1$ , respectively. Let  $H \leq \text{PGU}(3, q)$  be the Singer group consisting of

the elements of  $\text{PGU}(3, q)$  fixing the triangle  $T$ . Then  $H$  has order  $q^2 - q + 1$ ; see [30] and [22]. Since  $\sigma \in H$ ,  $\text{ord}(\sigma) \mid (q^2 - q + 1)$  and  $\sigma$  satisfies Case (B3).

Elements satisfying Case (B3) do exist; see for instance [4, Lemma 4.4]. The number  $k$  of triangles  $T$  whose vertices  $Q_1, Q_2, Q_3$  are such that  $Q_i \in \text{PG}(2, q^6) \setminus \text{PG}(2, q^2)$  and there exists some  $\sigma \in \text{PGU}(3, q)$  stabilizing  $T$ , is equal to the index in  $\text{PGU}(3, q)$  of the normalizer  $N$  of  $H$ . By [30] and [22] (see Case (iv) in Theorem 2.1),  $|N| = 3(q^2 - q + 1)$ . Hence  $k = q^3(q + 1)^2(q - 1)/3$ . By direct computation,  $k$  is equal to the number of triangles  $T'$  whose vertices  $Q'_1, Q'_2, Q'_3$  are such that  $Q'_i \in \text{PG}(2, q^6) \setminus \text{PG}(2, q^2)$  and  $Q'_i \in \mathcal{H}_q$ ,  $i = 1, 2, 3$ . Therefore, it is not possible that  $P_1, P_2, P_3$  have coordinates in  $\mathbb{F}_{q^6} \setminus \mathbb{F}_{q^2}$  and  $P_1 \notin \mathcal{H}_q$ .

- The case that  $P_1$  has coordinates in  $\mathbb{F}_{q^4} \setminus \mathbb{F}_{q^2}$  cannot occur. In fact, since  $\Phi_{q^2}$  acts on  $\{P_1, P_2, P_3\}$ , if  $P_1 \in \text{PG}(2, \mathbb{F}_{q^4}) \setminus \text{PG}(2, \mathbb{F}_{q^2})$ , then up to reordering  $P_2 \in \text{PG}(2, \mathbb{F}_{q^4}) \setminus \text{PG}(2, \mathbb{F}_{q^2})$  and  $P_3 \in \text{PG}(2, q^2)$ . Let  $i, j \in \{1, 2, 3\}$ ,  $i \neq j$ . By [30, §2 p. 212] and [22, pp. 141-142], any power of  $\sigma$  either fixes the line  $P_i P_j$  pointwise or has no fixed points on  $P_i P_j \setminus \{P_i, P_j\}$ . Thus  $\sigma$  has long orbits on  $P_i P_j \setminus \{P_i, P_j\}$ . In particular,  $\text{ord}(\sigma)$  divides the number of  $\mathbb{F}_{q^2}$ -rational points of both  $P_1 P_2$  and  $P_1 P_3 \setminus \{P_3\}$ , a contradiction.

□

Throughout the paper, a nontrivial element of  $\text{PGU}(3, q)$  is said to be of type (A), (B), (B1), (B2), (B3), (C), (D), or (E), as given in Lemma 2.2. Moreover,  $G$  always stands for a subgroup of  $\text{PGU}(3, q)$ .

**Lemma 2.3.** *Let  $H$  be a normal subgroup of  $G$ . Let  $A$  be the set of points of  $\text{PG}(2, \bar{\mathbb{F}}_q)$  fixed by every element of  $H$ , and  $B = A \cap \mathcal{H}_q$ . Then  $G$  acts on  $B$  and on  $A \setminus B$ .*

**Lemma 2.4.** *Let  $H$  be a  $m$ -subgroup of  $\text{PGU}(3, q)$ , where  $m \notin \{2, 3\}$  is a prime divisor of  $q + 1$ . Then  $H$  is abelian. Also, the nontrivial elements of  $H$  are either of types (A) or (B1), and in the latter case the fixed triangle  $T$  is the same for every element of  $H$ . In addition, if  $H$  is a Sylow  $m$ -subgroup of  $\text{PGU}(3, q)$ , then the unique fixed points of  $H$  are the vertices of  $T$  and  $H$  is the direct product of two cyclic groups whose nontrivial elements are of type (A).*

*Proof.* Since  $p \notin \{2, 3\}$ , the maximum power of  $m$  dividing  $|\text{PGU}(3, q)|$  is a square, say  $m^{2s}$ . Let  $\mathcal{H}_q$  have equation (2.1), and define

(2.4)

$$K = \{\text{diag}(\lambda, \mu, 1) \mid \lambda^s = \mu^s = 1\} \cong \{\text{diag}(\lambda, 1, 1) \mid \lambda^s = 1\} \times \{\text{diag}(1, \mu, 1) \mid \mu^s = 1\}.$$

Then  $K$  is an abelian Sylow  $m$ -subgroup of  $\text{PGU}(3, q)$ , whose fixed points are the fundamental points. Also, the nontrivial elements of  $K$  are either of type (A) or (B1). Up to conjugation,  $H$  is contained in  $K$  and the claim follows. □

**Lemma 2.5.** *Let  $H$  be a  $m$ -subgroup of  $\mathrm{PGU}(3, q)$ , where  $m$  is an odd prime divisor of  $q - 1$ . Then  $H$  is abelian and the unique fixed points of  $H$  are the vertices of a triangle  $T$ .*

*Proof.* Let  $\mathcal{H}_q$  have equation (2.2), and define

$$(2.5) \quad K = \{\mathrm{diag}(a^{q+1}, a, 1) \mid a \in \mathbb{F}_{q^2}^*\}.$$

Then  $K$  is an abelian Sylow  $m$ -subgroup of  $\mathrm{PGU}(3, q)$ , and the nontrivial elements of  $K$  fix exactly the fundamental points. Up to conjugation,  $H$  is contained in  $K$  and the claim follows.  $\square$

**Lemma 2.6.** *Let  $p \in \{2, 3\}$ . If  $G$  has a nontrivial normal subgroup  $H$  of prime order other than  $p$ , then  $p^2 \nmid |G|$ .*

*Proof.* Assume by contradiction that  $p^2 \mid |G|$  and let  $\sigma \in H$ . By Lemma 2.2, the type of  $\sigma$  is either (A) or (B). Suppose that  $\sigma$  is of type (A). Then, since  $H = \langle \sigma \rangle$ , all nontrivial elements of  $H$  are of type (A) and they have the same center  $P$  and axis  $\ell$ . On the other hand, by Lemma 2.3, any  $p$ -element of  $G$  fixes  $P$  and acts on  $\ell$ ; a contradiction by Lemma 2.2. Suppose that  $\sigma$  is of type (B). Then, since  $H = \langle \sigma \rangle$ , all nontrivial elements of  $H$  are of type (B) and they fix the same triangle  $T$ . By Lemma 2.3,  $G$  preserves  $T$ . Hence, by the orbit-stabilizer theorem, the elements of  $G$  fixing  $T$  pointwise form a subgroup  $M$  of index 1, 2, or 3. In all cases,  $M$  contains a  $p$ -element of type (A) or type (B), a contradiction by Lemma 2.2.  $\square$

From Function field theory we need the Riemann-Hurwitz formula; see [37, Theorem 3.4.13]. Every subgroup  $G$  of  $\mathrm{PGU}(3, q)$  produces a quotient curve  $\mathcal{H}_q/G$ , and the cover  $\mathcal{H}_q \rightarrow \mathcal{H}_q/G$  is a Galois cover defined over  $\mathbb{F}_{q^2}$  where the degree of the different divisor  $\Delta$  is given by the Riemann-Hurwitz formula, namely  $\Delta = (2g(\mathcal{H}_q) - 2) - |G|(2g(\mathcal{H}_q/G) - 2)$ . On the other hand,  $\Delta = \sum_{\sigma \in G \setminus \{id\}} i(\sigma)$ , where  $i(\sigma) \geq 0$  is given by the Hilbert's different formula [37, Thm. 3.8.7], namely

$$(2.6) \quad i(\sigma) = \sum_{P \in \mathcal{H}_q(\bar{\mathbb{F}}_q)} v_P(\sigma(t) - t),$$

where  $t$  is a local parameter at  $P$ .

By analyzing the geometric properties of the elements  $\sigma \in \mathrm{PGU}(3, q)$ , it turns out that there are only a few possibilities for  $i(\sigma)$ . This is obtained as a corollary of Lemma 2.2 and stated in the following proposition.

**Theorem 2.7.** *For a nontrivial element  $\sigma \in \mathrm{PGU}(3, q)$  one of the following cases occurs.*

- (1) *If  $\mathrm{ord}(\sigma) = 2$  and  $2 \mid (q + 1)$ , then  $\sigma$  is of type (A) and  $i(\sigma) = q + 1$ .*
- (2) *If  $\mathrm{ord}(\sigma) = 3$ ,  $3 \mid (q + 1)$  and  $\sigma$  is of type (B3), then  $i(\sigma) = 3$ .*
- (3) *If  $\mathrm{ord}(\sigma) \neq 2$ ,  $\mathrm{ord}(\sigma) \mid (q + 1)$  and  $\sigma$  is of type (A), then  $i(\sigma) = q + 1$ .*
- (4) *If  $\mathrm{ord}(\sigma) \neq 2$ ,  $\mathrm{ord}(\sigma) \mid (q + 1)$  and  $\sigma$  is of type (B1), then  $i(\sigma) = 0$ .*
- (5) *If  $\mathrm{ord}(\sigma) \mid (q^2 - 1)$  and  $\mathrm{ord}(\sigma) \nmid (q + 1)$ , then  $\sigma$  is of type (B2) and  $i(\sigma) = 2$ .*



- (6) If  $\text{ord}(\sigma) \neq 3$  and  $\text{ord}(\sigma) \mid (q^2 - q + 1)$ , then  $\sigma$  is of type (B3) and  $i(\sigma) = 3$ .
- (7) If  $p = 2$  and  $\text{ord}(\sigma) = 4$ , then  $\sigma$  is of type (D) and  $i(\sigma) = 2$ .
- (8) If  $\text{ord}(\sigma) = p$ ,  $p \neq 2$  and  $\sigma$  is of type (D), then  $i(\sigma) = 2$ .
- (9) If  $\text{ord}(\sigma) = p$  and  $\sigma$  is of type (C), then  $i(\sigma) = q + 2$ .
- (10) If  $\text{ord}(\sigma) \neq p$ ,  $p \mid \text{ord}(\sigma)$  and  $\text{ord}(\sigma) \neq 4$ , then  $\sigma$  is of type (E) and  $i(\sigma) = 1$ .

*Proof.* Suppose  $p \nmid \text{ord}(\sigma)$ . Then by [23, Theorem 11.74]  $i(\sigma)$  equals the number of points of  $\mathcal{H}_q$  fixed by  $\sigma$ . Also, for  $q$  odd all involutions are conjugated and are of type (A), by [27, Lemma 2.2 (ii)]. Therefore Cases (1) - (6) follow from Lemma 2.2.

Suppose  $\text{ord}(\sigma) = p$ , or  $p = 2$  and  $\text{ord}(\sigma) = 4$ . As in the proof of Lemma 2.2, we can assume that  $\sigma$  has the form  $\tau_{1,b,c}$  defined in (2.3). By direct computation,  $\sigma$  is of type (C) or (D) if and only if  $b = 0$  or  $b \neq 0$ , respectively. By [14, Eq. (2.12)],  $b = 0$  or  $b \neq 0$  if and only if  $i(\sigma) = q + 2$  or  $i(\sigma) = 2$ , respectively. From this, Cases (8) and (9) follow. Since  $(p, \text{ord}(\tau_{1,b,c})) = (2, 4)$  implies  $b \neq 0$ , Case (7) follows as well.

Suppose  $p \mid \text{ord}(\sigma)$ ,  $\text{ord}(\sigma) \neq p$ , and  $\text{ord}(\sigma) \neq 4$ . By [30, §2 p. 212] and [22, pp. 141-142],  $\sigma$  is of type (E). Let  $P \in \mathcal{H}_q$  be the unique fixed point of  $\sigma$  on  $\mathcal{H}_q$ . By [23, Theorem 11.74],  $\sigma$  is in the stabilizer of  $P$  but is not a  $p$ -element. Hence  $i(\sigma) = 1$ . Since Cases (A) - (E) in Lemma 2.2 cover all nontrivial elements of  $\text{PGU}(3, q)$ , Cases (1) - (10) give a complete classification.  $\square$

Theorem 2.7 extends [7, Lemma 4.1], where the result is for  $\sigma$  fixing an  $\mathbb{F}_{q^2}$ -rational point of  $\mathcal{H}_q$ .

Groups fixing an  $\mathbb{F}_{q^2}$ -rational point of  $\mathcal{H}_q$  are investigated in [14].

**Theorem 2.8.** [14, Thm. 3.3 and Eq. (2.12)] *Let  $p = 2$ . For a positive integer  $g$ , the following assertions are equivalent.*

- (1) *There exists a 2-subgroup  $G \leq \text{PGU}(3, q)$  such that  $g = g(\mathcal{H}_q/G)$ .*
- (2)  *$g = 2^{n-v-1}(2^{n-w} - 1)$  with  $0 \leq v \leq n - 1$  and  $0 \leq w \leq n - 1$ , and there exist additive subgroups  $V \subseteq \mathbb{F}_{q^2}$  and  $W \subseteq \mathbb{F}_q$  of order  $\text{ord}(V) = 2^v$  and  $\text{ord}(W) = 2^w$ , such that  $V^{q+1} = \{b^{q+1} \mid b \in V\}$  is contained in  $W$ .*

Assume that assertions (1) and (2) hold, and let  $\mathcal{H}_q$  have equation (2.2). Up to conjugation the unique point of  $\mathcal{H}_q$  fixed by every element of  $G$  is  $P_\infty = (1, 0, 0)$ , and the elements of  $G$  have the form (2.3). Then  $|G| = 2^{v+w}$  and the additive subgroups  $\{b \in \mathbb{F}_{q^2} \mid \tau_{1,b,c} \in G\} \leq \mathbb{F}_{q^2}$  and  $\{c \in \mathbb{F}_{q^2} \mid \tau_{1,0,c} \in G\} \leq \mathbb{F}_q$  have order  $2^v$  and  $2^w$ , respectively. In particular, the number of involutions of  $G$  equals  $2^w - 1$ .

**Theorem 2.9.** [14, Thm. 4.4 and Eq. (2.12)] *Let  $G$  fix an  $\mathbb{F}_{q^2}$ -rational point  $P \in \mathcal{H}_q$ , and let  $|G| = m \cdot p^u$  with  $m > 1$ ,  $m$  coprime with  $p$ . Then  $\mathcal{H}_q/G$  has genus*

$$g(\mathcal{H}_q/G) = \frac{(q - p^w)(q - (\gcd(m, q + 1) - 1)p^v)}{2mp^u},$$

where  $v, w$  are non-negative integers such that  $v + w = u$ .

Assume that  $G$  satisfies the hypotheses of Theorem 2.9 and let  $\mathcal{H}_q$  have equation (2.2). Up to conjugation  $P = (1, 0, 0)$  and the elements of  $G$  have the form

$$\tau_{a,b,c} = \begin{pmatrix} a^{q+1} & b^q & c \\ 0 & a & b \\ 0 & 0 & 1 \end{pmatrix},$$

with  $a, b, c \in \mathbb{F}_{q^2}$ ,  $a \neq 0$ ,  $b^{q+1} = c^q + c$ . Then the additive subgroups  $\{b \in \mathbb{F}_{q^2} \mid \tau_{1,b,c} \in G\}$  and  $\{c \in \mathbb{F}_{q^2} \mid \tau_{1,0,c} \in G\}$  of  $\mathbb{F}_{q^2}$  have order  $p^v$  and  $p^w$ , respectively. In particular, the number of nontrivial elements  $\sigma \in G$  with  $i(\sigma) = q + 2$  equals  $p^w - 1$ .

As a consequence of Theorem 2.7, the following result is obtained.

**Proposition 2.10.** *The Suzuki curve  $\mathcal{S}_2$  is a Galois subcover of the Hermitian curve  $\mathcal{H}_4$ .*

*Proof.* The Suzuki curve  $\mathcal{S}_2$  has genus 1 and is  $\mathbb{F}_{16}$ -maximal. Let  $G \leq \text{PGU}(3, 4)$  be a cyclic group of order 4. By Theorem 2.7, the  $\mathbb{F}_{16}$ -maximal quotient curve  $\mathcal{H}_4/G$  is elliptic. By [26, Thm. 77], there is only one  $\mathbb{F}_{16}$ -isomorphism class of  $\mathbb{F}_{16}$ -maximal elliptic curves. Then  $\mathcal{S}_2$  is  $\mathbb{F}_{16}$ -isomorphic to  $\mathcal{H}_4/G$ .  $\square$

Throughout the rest of the paper,  $C_r$  stands for a cyclic group of order  $r$ ,  $S_m$  is a Sylow  $m$ -subgroup of  $G$ , and  $n_m$  is the number of Sylow  $m$ -subgroups of  $G$ .

### 3. PROOF OF THEOREM 1.1

By absurd, let  $G \leq \text{PGU}(3, 64)$  be such that  $\mathcal{S}_8 \cong \mathcal{H}_{64}/G$ . The order of  $\text{PGU}(3, 64)$  is equal to  $2^{18} \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 13^2 \cdot 37 \cdot 109$ . From the Riemann-Hurwitz formula,

$$44 < \frac{|\mathcal{H}_{64}(\mathbb{F}_{8^4})|}{|\mathcal{S}_8(\mathbb{F}_{8^4})|} \leq |G| \leq \frac{2g(\mathcal{H}_{64}) - 2}{2g(\mathcal{S}_8) - 2} \leq 155.$$

Since  $|G|$  divides  $|\text{PGU}(3, 64)|$ ,

$$|G| \in \{45, 48, 50, 52, 56, 60, 63, 64, 65, 70, 72, 74, 75, 78, 80, 84, 90, 91, 96, \\ 100, 104, 105, 109, 111, 112, 117, 120, 126, 128, 130, 140, 144, 148, 150\}.$$

The different divisor has degree

$$(3.1) \quad \Delta = (2g(\mathcal{H}_{64}) - 2) - |G|(2g(\mathcal{S}_8) - 2) = 4030 - 26 \cdot |G|.$$

**Case  $|G| = 45$ .** By Sylow's Third Theorem [34, Thm. 6.10] and Schur-Zassenhaus Theorem [34, Thm. 9.19],  $G$  is the direct product  $G = S_3 \times C_5$ . Then  $G$  has 4 elements of order 5 and 40 elements of odd order multiple of 3. By Theorem 2.7,  $\Delta \leq 4 \cdot 65 + 40 \cdot 2$ , contradicting (3.1).

**Case  $|G| = 48$ .** Any group of order 48 has a normal subgroup of order 8 or 16 (see [35, p. 154 Ex. 10]); hence  $G$  has a normal 2-subgroup  $N$ . By [23, Theorem 11.74],  $N$  has a unique fixed point  $P$  on  $\mathcal{H}_{64}$ , which is  $\mathbb{F}_{64^2}$ -rational. By Lemma 2.3,  $G$  fixes  $P$ . From Theorem 2.9,

$$14 = \frac{(64 - 2^w)(64 - (\gcd(3, 65) - 1)2^v)}{2 \cdot 48},$$

with  $v + w = 4$ . By direct computation, this is not possible.

**Case  $|G| = 50$ .** By Sylow's Third Theorem and Schur-Zassenhaus Theorem,  $G$  is a semidirect product  $G = S_5 \rtimes C_2$ . By Theorem 2.7,  $\Delta = i \cdot 65 + (24 - i) \cdot 0 + n_2 \cdot 66 + (25 - n_2) \cdot 1$  with  $0 \leq i \leq 24$  and  $n_2 \in \{1, 5, 25\}$ . This contradicts (3.1).

**Case  $|G| = 52$ .** By Sylow's Third Theorem,  $n_{13} = 1$ . This contradicts Lemma 2.6.

**Case  $|G| = 56$ .** By Sylow's Third Theorem,  $n_2 = 1$  or  $n_7 = 1$ . Suppose that  $n_2 = 1$ , so that  $G = S_2 \rtimes C_7$ . Then  $S_2$  fixes an  $\mathbb{F}_{64^2}$ -rational point  $P \in \mathcal{H}_{64}$ , and  $G$  fixes  $P$  by Lemma 2.3. By Theorem 2.9,

$$14 = \frac{(64 - 2^w)(64 - (\gcd(7, 65) - 1)2^v)}{2 \cdot 56},$$

with  $v + w = 2$ ; this is a contradiction. The case  $n_7 = 1$  is impossible by Lemma 2.6.

**Case  $|G| = 60$ .** By [34, Problem 6.16], either  $n_5 = 1$  or  $G$  is isomorphic to the alternating group  $Alt(5)$ . The case  $n_5 = 1$  is impossible by Lemma 2.6; hence  $G \cong Alt(5)$ . By Theorem 2.7,  $\Delta = 15 \cdot 66 + 20 \cdot 2 + i \cdot 65 + (24 - i) \cdot 0$ , with  $0 \leq i \leq 24$ . This contradicts (3.1).

**Case  $|G| = 63$ .** By Theorem 2.7,  $\Delta = 62 \cdot 2$ , contradicting (3.1).

**Case  $|G| = 64$ .** By Theorem 2.8,  $14 = 2^{6-v-1}(2^{6-w} - 1)$  with  $0 \leq v, w \leq 5$ . Hence,  $v = 4$  and  $w = 3$ . Then, by Theorem 2.8 and Lemma 2.2,  $G$  has 7 elements of type (C) and 56 elements of type (D). By Theorem 2.7,  $\Delta = 7 \cdot 66 + 56 \cdot 2$ . This contradicts (3.1).

**Case  $|G| = 65$ .** By Lemma 2.2, any nontrivial element  $\sigma \in G$  is either of type (A) or of type (B1). If a generator of the cyclic group  $G$  is of type (A), then any element is of type (A) and  $\Delta = 64 \cdot 65$  by Theorem 2.7, contradicting (3.1). If the 48 generators of  $G$  are of type (B1), then  $\Delta \leq 16 \cdot 65$  by Theorem 2.7. This contradicts (3.1).

**Case  $|G| = 70$ .** By Sylow's Third Theorem,  $n_5 = n_7 = 1$  and  $n_2 \in \{1, 5, 7, 35\}$ ; hence,  $G = C_{35} \rtimes C_2$ . By Theorem 2.7,  $\Delta = n_2 \cdot 66 + (35 - n_2) \cdot 1 + 30 \cdot 2 + i \cdot 65 + (4 - i) \cdot 0$  with  $0 \leq i \leq 4$ . This contradicts (3.1).

**Case  $|G| = 72$ .** By [36, Theorem 1],  $G$  has a characteristic 3-subgroup  $N$ . By Lemma 2.5, the elements of  $N$  are of type (B2) with a common fixed triangle  $T$ . By Lemma 2.3,  $G$  acts on  $T$ . By the orbit-stabilizer theorem,  $G$  contains a 2-element fixing  $T$  pointwise, contradicting Lemma 2.2.

**Case  $|G| = 74$ .** For any prime power  $q$ ,  $PSU(3, q)$  has index  $\gcd(3, q + 1)$  in  $PGU(3, q)$ . This implies that, for any maximal subgroup  $M \neq PSU(3, q)$  of  $PGU(3, q)$ ,  $|M|$  divides

three times the order of a maximal subgroup of  $\text{PSU}(3, q)$ . By Theorem 2.1, 74 does not divide three times the order of any maximal subgroup of  $\text{PSU}(3, 64)$ , a contradiction.

**Case  $|G| = 75$ .** By Sylow and Schur-Zassenhaus theorems,  $G$  is a semidirect product  $G = S_5 \rtimes C_3$ . By Theorem 2.7,  $\Delta = i \cdot 65 + (24 - i) \cdot 0 + j \cdot 2 + (50 - j) \cdot 3$  with  $0 \leq i \leq 24$  and  $0 \leq j \leq 50$ . This contradicts (3.1).

**Case  $|G| = 78$ .** By Sylow's Third Theorem,  $n_{13} = 1$ ; by Lemma 2.3,  $G$  acts on the fixed points of  $S_{13}$ . Every nontrivial element  $\sigma \in S_{13}$  generates  $S_{13}$  and is either of type (A) or (B1). Hence, all nontrivial elements of  $G$  either are of type (A), or act on a common triangle  $T$ . In the former case,  $G$  contains a 2-element of type (A), contradicting Lemma 2.2. In the latter case, by the orbit-stabilizer theorem, the subgroup  $H$  of  $G$  fixing  $T$  pointwise contains a 2-element or a 3-element. This contradicts Lemma 2.2.

**Case  $|G| = 80$ .** By [36, Theorem 1],  $G$  has a characteristic 2-subgroup  $N$ . By Lemma 2.3,  $G$  fixes the unique fixed point of  $N$  on  $\mathcal{H}_{64}$ , which is  $\mathbb{F}_{64^2}$ -rational. By Theorem 2.9,

$$14 = \frac{(64 - 2^w)(64 - (\gcd(5, 65) - 1)2^v)}{2 \cdot 80},$$

with  $v + w = 4$ , which is impossible.

**Case  $|G| = 84$ .** By Sylow's Third Theorem,  $n_7 = 1$ . This contradicts Lemma 2.6.

**Case  $|G| = 90$ .** Since  $|G| \equiv 2 \pmod{4}$ ,  $G$  has a normal subgroup  $N$  of index 2 (see [31, Ex. 4.3]). By Sylow's Third Theorem,  $N$  has a characteristic 5-subgroup  $C_5$ , so that  $C_5$  is normal in  $G$  and  $n_5 = 1$ . Also,  $n_3 = 1$ . Then  $G$  is a semidirect product  $G = C_5 \times S_3 \rtimes C_2$ . By Theorem 2.7,  $\Delta = 4 \cdot i + 40 \cdot 2 + n_2 \cdot 66 + (45 - n_2) \cdot 1$ , with  $i \in \{0, 65\}$  and  $1 < n_2 \mid 45$ . This contradicts (3.1).

**Case  $|G| = 91$ .** By Theorem 2.7,  $\Delta = 78 \cdot 2 + 12 \cdot i$  with  $i \in \{0, 65\}$ , contradicting (3.1).

**Case  $|G| = 96$ .** By [36, Theorem 1],  $G$  has a characteristic 2-subgroup  $N$ . By Lemma 2.3,  $G$  fixes the unique fixed point of  $N$  on  $\mathcal{H}_{64}$ , which is  $\mathbb{F}_{64^2}$ -rational. By Theorem 2.9,

$$14 = \frac{(64 - 2^w)(64 - (\gcd(3, 65) - 1)2^v)}{2 \cdot 91},$$

with  $v + w = 5$ , which is impossible.

**Case  $|G| = 100$ .** By Sylow's Third Theorem,  $n_5 = 1$ . By Lemma 2.4, the fixed points of  $S_5$  are the vertices of a triangle  $T$ . By Lemma 2.3,  $G$  acts on  $T$ . By the orbit-stabilizer theorem,  $G$  contains a 2-element fixing  $T$  pointwise. This contradicts Lemma 2.2.

**Case  $|G| = 104$ .** By Sylow's Third Theorem,  $n_{13} = 1$ . This contradicts Lemma 2.6.

**Case  $|G| = 105$ .** By Sylow's Third Theorem,  $n_5 \in \{1, 21\}$ . All elements of a  $S_5$  are of the same type, either (A) or (B1). Then, by Theorem 2.7,  $\Delta = 4i \cdot 65 + 4(n_5 - i) \cdot 0 + (104 - 4n_5) \cdot 2$ , with  $0 \leq i \leq n_5$ . This contradicts (3.1).

**Case  $|G| = 109$ .** By Theorem 2.7,  $\Delta = 108 \cdot 3$ . This contradicts (3.1).

**Case  $|G| = 111$ .** By Sylow and Schur-Zassenhaus theorems,  $n_{37} = 1$ ,  $n_3 \in \{1, 37\}$ , and  $G$  is a semidirect product  $G = C_{37} \rtimes C_3$ . By Lemma 2.2,  $G$  has no elements of order  $37 \cdot 3$ . Hence,  $n_3 = 37$ . By Theorem 2.7,  $\Delta = 36 \cdot 3 + 74 \cdot 2$ . This contradicts (3.1).

**Case  $|G| = 112$ .** By [36, Theorem 1],  $G$  has a characteristic 2-subgroup  $N$ . By Lemma 2.3,  $G$  fixes the unique fixed point of  $N$  on  $\mathcal{H}_{64}$ , which is  $\mathbb{F}_{64^2}$ -rational. By Theorem 2.9,

$$14 = \frac{(64 - 2^w)(64 - (\gcd(7, 65) - 1)2^v)}{2 \cdot 112},$$

with  $v + w = 4$ , which is a contradiction.

**Case  $|G| = 117$ .** By Sylow and Schur-Zassenhaus theorems,  $G$  is a semidirect product  $G = C_{13} \rtimes S_3$ . Since 13 is prime, the nontrivial elements of  $C_{13}$  are of the same type (A) or (B1). By Theorem 2.7,  $\Delta = 12 \cdot i + 104 \cdot 2$  with  $i \in \{0, 65\}$ . Then  $i = 65$  by (3.1), i.e. the nontrivial elements of  $C_{13}$  are homologies, with a common center  $P \notin \mathcal{H}_{64}$  and axis  $\ell$ . By Lemma 2.3,  $G$  fixes  $P$  and acts on  $\ell$ . By Lemma 2.2, the nontrivial elements of  $S_3$  are of type (B2) and fix two  $\mathbb{F}_{64^2}$ -rational points  $Q, R \in \ell \cap \mathcal{H}_{64}$ . Let  $\mathcal{H}_{64}$  have equation (2.2). Since  $\text{PGU}(3, q)$  is 2-transitive on the  $\mathbb{F}_{64^2}$ -rational points of  $\mathcal{H}_{64}$ , we can assume that  $Q = (1, 0, 0)$  and  $R = (0, 0, 1)$ . Then  $C_{13} = \{\text{diag}(1, \lambda, 1) \mid \lambda^{13} = 1\}$  and  $S_3 = \{\text{diag}(a^{65}, a, 1) \mid a^9 = 1\} = C_9$ ; see [14]. Hence,  $G$  is abelian and is the direct product  $G = C_{13} \times C_9$ . Let  $\bar{G} \leq \text{PGU}(3, 64)$  be the group  $\bar{G} = C_{65} \times C_9$ , where  $C_{65}$  is generated by  $\text{diag}(1, \bar{\lambda}, 1)$ , with  $\bar{\lambda}$  a primitive 65-th root of unity. Then  $G$  is a normal subgroup of  $\bar{G}$  of index 5, so that  $\bar{G}/G \leq \text{Aut}(\mathcal{H}_{64}/G)$  has order 5. Also,  $\bar{G}/G$  has two  $\mathbb{F}_8$ -rational fixed points on  $\mathcal{H}_{64}/G$ , namely the points lying under  $Q$  and  $R$ . This is inconsistent with the structure of the automorphism group of  $\mathcal{S}_8$ . In fact, by [23, Theorem A.12] (see also [17, Remark (2.2)]), any subgroup of  $\text{Aut}(\mathcal{S}_8)$  of order 5 is a Singer group acting semiregularly on the  $\mathbb{F}_8$ -rational points of  $\mathcal{S}_8$ .

**Case  $|G| = 120$ .** By [31, Ex. 8.19], either  $n_5 = 1$ , or  $G$  has a normal 2-subgroup, or  $G$  is isomorphic to the symmetric group  $\text{Sym}(5)$ . The case  $n_5 = 1$  is impossible by Lemma 2.6. Hence,  $n_5 = 6$ . Suppose that  $G$  has a normal 2-subgroup  $N$ . By Lemma 2.3,  $G$  fixes the unique fixed point of  $N$  on  $\mathcal{H}_{64}$ . Then any 5-element of  $G$  is of type (A) by Lemma 2.2. By Theorem 2.7,  $\Delta \geq 24 \cdot 65$ ; this contradicts (3.1). Suppose that  $G \cong \text{Sym}(5)$ . Then  $G$  contains 25 involutions. By Theorem 2.7,  $\Delta \geq 25 \cdot 66$ . This contradicts (3.1).

**Case  $|G| = 126$ .** Since  $|G| \equiv 2 \pmod{4}$ ,  $G$  has a normal subgroup  $N$  of index 2. Then  $G$  is a semidirect product  $G = N \rtimes C_2$ . By Theorem 2.7,  $\Delta = 62 \cdot 2 + n_2 \cdot 66 + (63 - n_2) \cdot 1$ . This contradicts (3.1).

**Case  $|G| = 128$ .** By Theorem 2.1,  $G$  fixes an  $\mathbb{F}_{64^2}$ -rational point of  $\mathcal{H}_{64}$ . Then, by Theorem 2.8,  $14 = 2^{6-v-1}(2^{6-w} - 1)$  with  $0 \leq v, w \leq 5$ . Hence,  $v = 4, w = 3$ . By theorem 2.8,  $G$  contains exactly  $2^3 - 1$  involutions. By Theorem 2.7,  $\Delta = 7 \cdot 66 + 120 \cdot 1$ . This contradicts (3.1).

**Case  $|G| = 130$ .** By Sylow's Third Theorem,  $n_{13} = 1$ ,  $n_5 \in \{1, 26\}$ , and  $n_2 \in \{1, 5, 13, 65\}$ . By (3.1),  $\Delta = 650$ . Hence, by Theorem 2.7, the nontrivial elements of

$S_{13}$  are of type (B1). We remark that if  $x$  is an element of type (C) normalizing an element  $y$  of type (A) or (B1), then the element  $yx$  is of type (E). If  $n_5 = 1$ , then  $G$  is a semidirect product  $G = C_{65} \rtimes C_2$ ; hence,  $n_2 = 1$  by the above remark. If  $n_5 = 26$ , then  $G$  contains 12 elements of order 13,  $4 \cdot 26$  elements of order 5, and 12 elements of type (E) by the above remark. Hence,  $n_2 = 1$ . Therefore  $G$  contains a unique involution  $\sigma$ . By Lemma 2.3,  $S_{13}$  fixes the unique fixed point of  $\sigma$  on  $\mathcal{H}_{64}$ . This contradicts Lemma 2.2.

**Case**  $|G| = 140$ . By Sylow's Third Theorem,  $n_7 = 1$ . This contradicts Lemma 2.6.

**Case**  $|G| = 144$ . By Theorem 2.7,  $\Delta = i \cdot 66 + j \cdot 1 + k \cdot 2$  with  $i + j + k = 143$ . Here,  $i$  is the number of involutions in  $G$ ,  $j$  is the number of elements of order 6 or 18 in  $G$ , and  $k$  is the number of elements of order 3, 9, or 4 in  $G$ . Suppose  $i = 1$ . Then, by Lemma 2.3,  $G$  fixes the unique fixed point of the involution on  $\mathcal{H}_{64}$ , which is  $\mathbb{F}_{64^2}$ -rational. By Theorem 2.9,

$$14 = \frac{(64 - 2^w)(64 - (\gcd(9, 65) - 1)2^v)}{2 \cdot 144},$$

with  $v + w = 4$ , hence  $w = 0$ . By Theorem 2.9,  $G$  has no involutions, which is impossible. Then  $i \geq 2$  and thus by (3.1), we have  $i = 2$  and  $k = 13$ . This implies that  $G$  contains 2 involutions and at most 13 elements of order 4. Hence,  $G$  has a unique Sylow 2-subgroup  $S_2$ . Then, by Lemma 2.3,  $G$  fixes the unique fixed point of  $S_2$  on  $\mathcal{H}_{64}$  and as before, it leads to a contradiction by Theorem 2.9.

**Case**  $|G| = 148$ . By Theorem 2.1,  $|G|$  does not divide three times the order of any maximal subgroup of  $\text{PSU}(3, 64)$ . Hence,  $G$  is not contained in any maximal subgroup of  $\text{PGU}(3, 64)$ , a contradiction.

**Case**  $|G| = 150$ . By Lemma 2.4,  $G$  contains 8 elements of type (A). Hence, by Theorem 2.7,  $\Delta \geq 8 \cdot 65$ . This contradicts (3.1).

This completes the proof of Theorem 1.1.

It may be noticed in the above proof that the hypothesis  $g = 14$  together with the  $\mathbb{F}_{64^2}$ -maximality of  $\mathcal{S}_8$  were sufficient to get a contradiction for  $|G| \neq 117$ . Instead, a group  $G$  of order 117 with the required ramification exists, and we gave an explicit construction. Such a group  $G$  is uniquely determined up to conjugation. Using MAGMA [1], we found a plane model of  $\mathcal{H}_{64}/G$  over  $\mathbb{F}_2$ , as well as a non-singular model of  $\mathcal{H}_{64}/G$  in  $\text{PG}(13, 2)$ .

**Proposition 3.1.** *Let  $\mathcal{X}$  be an  $\mathbb{F}_{64^2}$ -maximal curve of genus 14. If  $\mathcal{X}$  is Galois covered by  $\mathcal{H}_{64}$  then  $\mathcal{X} \cong \mathcal{H}_{64}/G$  where  $G$  is a cyclic group  $G \leq \text{PGU}(3, 64)$  of order 117, and a plane model of  $\mathcal{X}$  over  $\mathbb{F}_2$  is the (singular) plane curve*

$$X^7 Y^5 + X + Y^5 = 0,$$

*while a nonsingular model in  $\mathbb{P}^{13}$  of  $\mathcal{X}$  over  $\mathbb{F}_2$  is the image of  $\mathcal{X}$  under the morphism*

$$\varphi : \mathcal{X} \rightarrow \mathbb{P}^{13}, \quad (x, y, 1) \mapsto (x, y, xy, x^2 y, y^2, xy^2, x^2 y^2, x^3 y^2, y^3, xy^3, x^2 y^3, x^3 y^3, x^4 y^3, 1).$$

## 4. PROOF OF THEOREM 1.2

By absurd, let  $\mathcal{R}_3 \cong \mathcal{H}_{27}/G$  for  $G \leq \text{PGU}(3, 27)$ . The order of  $\text{PGU}(3, 27)$  is equal to  $2^5 \cdot 3^9 \cdot 7^2 \cdot 13 \cdot 19 \cdot 37$ . From the Riemann-Hurwitz formula,

$$12 < \frac{|\mathcal{H}_{27}(\mathbb{F}_{27^2})|}{|\mathcal{R}_3(\mathbb{F}_{27^2})|} \leq |G| \leq \frac{2g(\mathcal{H}_{27}) - 2}{2g(\mathcal{R}_3) - 2} \leq 25.$$

Since  $|G|$  divides  $|\text{PGU}(3, 27)|$ ,

$$|G| \in \{13, 14, 16, 18, 19, 21, 24\}.$$

The different divisor has degree

$$(4.1) \quad \Delta = (2g(\mathcal{H}_{27}) - 2) - |G|(2g(\mathcal{R}_3) - 2) = 700 - 28 \cdot |G|.$$

**Case**  $|G| = 13$ . By Theorem 2.7,  $\Delta = 12 \cdot 2$ . This contradicts (4.1).

**Case**  $|G| = 14$ . By Sylow and Schur-Zassenhaus theorems,  $G$  is a semidirect product  $G = C_7 \rtimes C_2$ . All nontrivial elements of  $C_7$  are of the same type, which is either (A) or (B1) by Lemma 2.2. Therefore, by Theorem 2.7,  $\Delta = 6 \cdot i + 7 \cdot 28$ , with  $i \in \{0, 28\}$ . This contradicts (4.1).

**Case**  $|G| = 16$ .  $\text{PGU}(3, 27)$  has just three conjugacy classes of subgroups of order 16, which are isomorphic either to the Iwasawa group  $M_{16} = \langle x, y \mid x^8 = y^2 = 1, yxy^{-1} = x^5 \rangle$ , or to the direct product  $C_4 \times C_4$ , or to the central product  $D_8 \circ C_4 = \langle \alpha, \beta, \gamma \mid \alpha^4 = \beta^2 = 1, \beta\alpha\beta^{-1} = \alpha^{-1}, \alpha^2 = \gamma^2, \alpha\gamma = \gamma\alpha, \beta\gamma = \gamma\beta \rangle$ .

Suppose  $G \cong M_{16}$ . By MAGMA computation, the normalizer  $N$  of  $G$  in  $\text{PGU}(3, 27)$  has order 224, and the quotient group  $N/G \leq \text{Aut}(\mathcal{H}_{27}/G)$  is a cyclic group of order 14. On the other hand, the subgroups of  $\text{Ree}(3) \cong \text{P}\Gamma\text{L}(2, 8)$  of order 14 are not abelian, a contradiction.

Suppose  $G \cong C_4 \times C_4$ . By MAGMA computation, the normalizer  $N$  of  $G$  in  $\text{PGU}(3, 27)$  has order 4704. Hence, the group  $N/G \leq \text{Aut}(\mathcal{H}_{27}/G)$  has order 294, which does not divide the order of  $\text{Ree}(3)$ . This contradicts  $\mathcal{H}_{27}/G \cong \mathcal{R}_3$ .

Suppose  $G \cong D_8 \circ C_4$ . By MAGMA computation, the normalizer  $N$  of  $G$  in  $\text{PGU}(3, 27)$  has order 672, and the group  $N/G \leq \text{Aut}(\mathcal{H}_{27}/G)$  is isomorphic to  $C_{21} \rtimes C_2$ . On the other hand, the subgroups of  $\text{Ree}(3)$  of order 42 have no cyclic subgroups of order 21, a contradiction.

**Case**  $|G| = 18$ . By Sylow's Third Theorem,  $n_3 = 1$ . By [23, Theorem 11.74],  $S_3$  has a unique fixed point  $P$  on  $\mathcal{H}_{27}$ , which is  $\mathbb{F}_{27^2}$ -rational. By Lemma 2.3,  $G$  fixes  $P$ . Then, by Theorem 2.9,

$$15 = \frac{(27 - 3^w)(27 - (\gcd(2, 28) - 1)3^v)}{2 \cdot 18},$$

with  $v + w = 2$ , which is impossible.

**Case**  $|G| = 19$ . By Theorem 2.7,  $\Delta = 18 \cdot 3$ . This contradicts (4.1).

**Case  $|G| = 21$ .** By Sylow and Schur-Zassenhaus theorems,  $G$  is a semidirect product  $G = C_7 \rtimes C_3$ . All nontrivial elements of  $C_7$  are of the same type, which is either (A) or (B1) by Lemma 2.2. Thus, by Theorem 2.7,  $\Delta = 6 \cdot i + 2n_3 \cdot 29 + (14 - 2n_3) \cdot 1$ , with  $i \in \{0, 28\}$ . This contradicts (4.1).

**Case  $|G| = 24$ .** Since  $3 \mid |G|$ , we have  $\Delta \geq 29$  by Theorem 2.7. This contradicts (4.1).

This completes the proof of Theorem 1.2.

It may be noticed in the above proof that the hypothesis  $g = 15$  together with the  $\mathbb{F}_{27^2}$ -maximality of  $\mathcal{R}_3$  ruled out all cases but  $|G| = 16$ . For this exception, three cases are treated separately.

- $G \cong M_{16}$ . Then  $G$  contains 3 involutions, 4 elements of order 4, and 8 elements of order 8. By Theorem 2.7, the quotient curve  $\mathcal{H}_{27}/G$  has genus 18.
- $G \cong C_4 \times C_4$ . By the Riemann-Hurwitz formula,  $\mathcal{H}_{27}/G$  has genus 15. Also,  $G$  has 9 elements of type (A) and 6 elements of type (B1). Hence,  $G$  fixes the vertices of a triangle  $T$ . Let  $\mathcal{H}_{27}$  have equation (2.1). Up to conjugation,  $T$  is the fundamental triangle and  $G = \{\text{diag}(\lambda, \mu, 1) \mid \lambda^4 = \mu^4 = 1\}$ . Therefore a (singular) plane model of  $\mathcal{H}_{27}/G$  is  $X^7 + Y^7 + 1 = 0$ .
- $G \cong D_8 \circ C_4$ . By the Riemann-Hurwitz formula,  $\mathcal{H}_{27}/G$  has genus 15. Also,  $G$  contains 9 elements of type (A) and 6 elements of type (B1). In particular, the non-central involutions of  $D_8$  are non-commuting elements of type (A). Thus, the generator  $y$  of the center  $C_4$  is not of type (B1). Hence,  $y$  is of type (A). Let  $\mathcal{H}_{27}$  have equation (2.1). Up to conjugation, the generators of  $G$  are  $\alpha : (X, Y, T) \mapsto (Y, -X, T)$ ,  $\beta = \text{diag}(1, -1, 1)$ , and  $\gamma = \text{diag}(\lambda, \lambda, 1)$ , where  $\lambda^2 = -1$ . A plane model of  $\mathcal{H}_{27}/G$  is obtained by MAGMA computation, as follows.

**Proposition 4.1.** *Let  $\mathcal{X}$  be an  $\mathbb{F}_{27^2}$ -maximal curve of genus 15. If  $\mathcal{X}$  is Galois covered by  $\mathcal{H}_{27}$  then  $\mathcal{X} \cong \mathcal{H}_{27}/G$  where  $G \leq \text{PGU}(3, 27)$  has order 16, and one of the following cases occurs.*

- $G \cong C_4 \times C_4$  and a plane model for  $\mathcal{X}$  is given by the affine equation

$$X^7 + Y^7 + 1 = 0.$$

- $G \cong D_8 \circ C_4$  and a plane model for  $\mathcal{X}$  is given by the affine equation

$$X^{28} + X^{27} + X^{26} + 2X^{23} + 2X^{22} + X^{21} + 2X^{12}Y^{14} + X^{10}Y^{14} + 2X^7Y^{14} + Y^{28} = 0.$$

## 5. GALOIS SUBCOVERS OF $\mathcal{H}_{27}$

Theorem 5.1 shows the complete spectrum of genera of Galois subcovers of  $\mathcal{H}_{27}$ , consisting of integers  $g$  which are the genera of a quotient curve  $\mathcal{H}_{27}/G$  with  $G$  ranging on the set of all subgroups of  $\text{PGU}(3, 27)$ .



**Theorem 5.1.** *The spectrum of genera of Galois subcovers of  $\mathcal{H}_{27}$  is*

$$\Sigma_{27} = \{0, 1, 3, 4, 5, 6, 7, 9, 10, 12, 13, 15, 16, 17, 18, 19, 24, 25, \\ 26, 27, 36, 39, 43, 51, 52, 78, 85, 108, 117, 169, 351\}.$$

The proof relies on the results of Section 2. A case-by-case analysis of all integers  $g$  with  $1 < g \leq g(\mathcal{H}_{27})$  is combined with

$$(5.1) \quad \frac{19684}{730 + 54g} = \frac{|\mathcal{H}_{27}(\mathbb{F}_{27^2})|}{|\mathcal{H}_{27}/G(\mathbb{F}_{27^2})|} \leq |G| \leq \frac{2g(\mathcal{H}_{27}) - 2}{2g(\mathcal{H}_{27}/G) - 2} = \frac{700}{2g - 2},$$

which bounds the order of a putative group  $G \leq \text{PGU}(3, 27)$  such that  $\mathcal{H}_{27}/G$  has genus  $g$ . This leads us to look inside the structure of the groups  $G$  satisfying (5.1) and compute the genus of  $\mathcal{H}_{27}/G$ , for  $g > 1$ . These results are summarized in Theorem 5.1. For each  $g > 1$  in  $\Sigma_{27}$ , Tables 1 and 2 provide a classification of the groups  $G$  for which  $\mathcal{H}_{27}/G$  has genus  $g$ .

TABLE 1. Quotient curves  $\mathcal{H}_{27}/G$  of genus  $g \geq 17$

$g$	$ G $	structure of $G$
351	1	trivial group.
169	2	$G = C_2 = \langle \sigma \rangle$ , $\sigma$ of type (A).
117	3	$G = C_3 = \langle \sigma \rangle$ , $\sigma$ of type (D).
108	3	$G = C_3 = \langle \sigma \rangle$ , $\sigma$ of type (C).
85	4	$G = C_4 = \langle \sigma \rangle$ , $\sigma$ of type (B1).
78	4	$G = C_4 = \langle \sigma \rangle$ , $\sigma$ of type (A).
52	6	$G = C_6 = \langle \sigma \rangle$ , $\sigma$ of type (E). $G = \text{Sym}(3) = \langle \alpha \rangle \rtimes \langle \beta \rangle$ , $\alpha$ of type (C), $\beta$ of type (A).
51	7	$G = C_7 = \langle \sigma \rangle$ , $\sigma$ of type (B1).
43	8	$G = Q_8$ quaternion group, 1 element of type (A), 6 elements of type (B1).
39	7	$G = C_7 = \langle \sigma \rangle$ , $\sigma$ of type (A).
	8	$G = C_8 = \langle \sigma \rangle$ , $\sigma$ of type (B2).
	9	$G = C_3 \times C_3 = \langle \alpha \rangle \times \langle \beta \rangle$ , $\alpha$ and $\beta$ of type (D).
36	8	$G = C_4 \times C_2 = \langle \alpha \rangle \times \langle \beta \rangle$ , $\alpha$ of type (B1), $\beta$ of type (A).
	8	$G = D_8$ dihedral group, involutions of type (A), 2 elements of type (B1).
	9	$G = C_3 \times C_3 = \langle \alpha \rangle \times \langle \beta \rangle$ , $\alpha$ of type (C), $\beta$ of type (D).
27	9	$G = C_3 \times C_3 = \langle \alpha \rangle \times \langle \beta \rangle$ , $\alpha$ and $\beta$ of type (C).
	13	$G = C_{13} = \langle \sigma \rangle$ , $\sigma$ of type (B2).
26	12	$G = \text{Alt}(4)$ , involutions of type (A), other elements of type (D).
25	14	$G = C_{14} = \langle \sigma \rangle$ , $\sigma$ of type (B1).
24	12	$G = C_{12} = \langle \sigma \rangle$ , $\sigma$ of type (E).
19	14	$G = C_{14} = \langle \sigma \rangle$ , $\sigma$ of type (B1), $\sigma^2$ of type (A).
18	16	$G = M_{16}$ , 5 elements of type (A), 2 elements of type (B1), 8 elements of type (B2).
18	19	$G = C_{19} = \langle \sigma \rangle$ , $\sigma$ of type (B3).
17	21	$G = C_7 \rtimes C_3 = \langle \alpha \rangle \rtimes \langle \beta \rangle$ , $\alpha$ of type (B1), $\beta$ of type (B2).

TABLE 2. Quotient curves  $\mathcal{H}_{27}/G$  of genus  $3 \leq g \leq 16$ 

$g$	$ G $	structure of $G$
16	18	$G = C_3 \times (C_3 \rtimes C_2) = \langle \alpha \rangle \times (\langle \beta \rangle \rtimes \langle \gamma \rangle)$ , $\alpha$ of type (C), $\beta$ of type (D), $\gamma$ of type (A).
15	16	$G = C_4 \times C_4 = \langle \alpha \rangle \times \langle \beta \rangle$ , $\alpha$ and $\beta$ of type (A).
	16	$G = D_8 \circ C_4 = (\langle \alpha \rangle \rtimes \langle \beta \rangle) \circ \langle \gamma \rangle$ , $\alpha$ of type (B1), $\beta$ and $\gamma$ of type (A).
13	14	$G = C_{14} = \langle \sigma \rangle$ , $\sigma$ of type (A).
	18	$G = C_3 \times (C_3 \rtimes C_2) = \langle \alpha \rangle \times (\langle \beta \rangle \rtimes \langle \gamma \rangle)$ , $\alpha$ and $\beta$ of type (D), $\gamma$ of type (A).
	18	$G = C_3 \times (C_3 \rtimes C_2) = \langle \alpha \rangle \times (\langle \beta \rangle \rtimes \langle \gamma \rangle)$ , $\alpha$ and $\beta$ of type (C), $\gamma$ of type (A).
	26	$G = C_{26} = \langle \sigma \rangle$ , $\sigma$ of type (E).
	27	$G = (C_3 \times C_3) \rtimes C_3 = (\langle \alpha \rangle \times \langle \beta \rangle) \rtimes \langle \gamma \rangle$ , $\alpha, \beta, \gamma$ of type (D).
	28	$G = C_{28} = \langle \sigma \rangle$ , $\sigma$ of type (B1), 1 element of type (A).
12	21	$G = C_{21} = \langle \sigma \rangle$ , $\sigma$ of type (E).
	24	$G = C_3 \rtimes C_8 = \langle \alpha \rangle \rtimes \langle \beta \rangle$ , $\alpha$ of type (C), $\beta$ of type (B2).
	27	$G = C_3 \times (C_3 \times C_3) = \langle \alpha \rangle \times (\langle \beta \rangle \times \langle \gamma \rangle)$ , $\alpha$ of type (C), $\beta$ and $\gamma$ of type (D).
	28	$G = C_{28} = \langle \sigma \rangle$ , $\sigma$ of type (B1), 3 elements of type (A).
	28	$G = C_{14} \times C_2 = \langle \alpha \rangle \times \langle \beta \rangle$ , $\alpha$ of type (B1), $\beta$ of type (A), 3 elements of type (A).
10	24	$G \cong \text{SL}(2, 3)$ , 1 element of type (A), 6 elements of type (B1), 8 elements of type (C), 8 elements of type (E).
9	37	$G = C_{37} = \langle \sigma \rangle$ , $\sigma$ of type (B3).
7	26	$G = C_{13} \rtimes C_2 = \langle \alpha \rangle \rtimes \langle \beta \rangle$ , $\alpha$ of type (B2), $\beta$ of type (A).
	28	$G = C_{28} = \langle \sigma \rangle$ , $\sigma$ of type (B1), 14 elements of type (A).
	52	$G = C_{13} \rtimes C_4 = \langle \alpha \rangle \rtimes \langle \beta \rangle$ , $\alpha$ of type (B2), $\beta$ of type (B1).
6	28	$G = C_{14} \times C_2 = \langle \alpha \rangle \times \langle \beta \rangle$ , $\alpha$ and $\beta$ of type (A), 15 elements of type (A).
	32	$G = C_4 \wr C_2 = \langle \alpha \rangle \wr \langle \beta \rangle$ wreath product, 13 elements of type (A), 10 elements of type (B1), 8 elements of type (B2).
	52	$G = C_{52} = \langle \sigma \rangle$ , $\sigma$ of type (B2), 3 elements of type (A).
	57	$G = C_{19} \rtimes C_3 = \langle \alpha \rangle \rtimes \langle \beta \rangle$ , $\alpha$ of type (B3), $\beta$ of type (D).
5	48	$G = (C_4 \times C_4) \rtimes C_3 = (\langle \alpha \rangle \times \langle \beta \rangle) \rtimes \langle \gamma \rangle$ , $\alpha$ and $\beta$ of type (A), $\gamma$ of type (D).
4	42	$G = C_{42} = \langle \sigma \rangle$ , $\sigma$ of type (E).
	48	$G = (D_8 \circ C_4) \rtimes \langle \sigma \rangle$ , $\sigma$ of type (C).
	54	$G = (C_3 \times C_3 \rtimes C_3) \rtimes \langle \sigma \rangle$ , $\sigma$ of type (A).
	56	$G = Q_8 \rtimes \langle \sigma \rangle$ , $\sigma$ of type (A).
	72	$G = C_4 \times C_2 \rtimes (\langle \alpha \rangle \times \langle \beta \rangle)$ , $\alpha$ and $\beta$ of type (D).
	81	$G = C_3 \times C_3 \times C_3 \times C_3 = \langle \alpha \rangle \times \langle \beta \rangle \times \langle \gamma \rangle \times \langle \delta \rangle$ , $\alpha, \beta, \gamma, \delta$ of type (D).
3	49	$G = C_7 \times C_7 = \langle \alpha \rangle \times \langle \beta \rangle$ , $\alpha$ and $\beta$ of type (A).
	56	$G = \langle \sigma \rangle \rtimes D_8$ , $\sigma$ of type (A).
	63	$G = C_7 \times C_3 \times C_3 = \langle \alpha \rangle \times \langle \beta \rangle \times \langle \gamma \rangle$ , $\alpha$ of type (A), $\beta$ and $\gamma$ of type (C).
	72	$G = C_3 \times C_3 \rtimes C_8 = \langle \alpha \rangle \times \langle \beta \rangle \rtimes \langle \gamma \rangle$ , $\alpha$ and $\beta$ of type (C), $\gamma$ of type (B2).
	81	$G = C_3 \times C_3 \times C_3 \times C_3 = \langle \alpha \rangle \times \langle \beta \rangle \times \langle \gamma \rangle \times \langle \delta \rangle$ , $\alpha, \beta$ of type (C), $\gamma, \delta$ of type (D).
	91	$G = C_{91} = \langle \sigma \rangle$ , $\sigma$ of type (B2).
	104	$G = C_{13} \rtimes C_8 = \langle \alpha \rangle \rtimes \langle \beta \rangle$ , $\alpha$ and $\beta$ of type (B2), or $G = C_{104} = \langle \sigma \rangle$ , $\sigma$ of type (B2).
	111	$G = C_{37} \rtimes C_3 = \langle \alpha \rangle \rtimes \langle \beta \rangle$ , $\alpha$ of type (B3), $\beta$ of type (D).
	112	$G = C_7 \times C_4 \times C_4 = \langle \alpha \rangle \times \langle \beta \rangle \times \langle \gamma \rangle$ , $\alpha$ of type (B1), $\beta$ and $\gamma$ of type (A).

Theorem 5.1 shows that some quotient curves of  $\mathcal{R}_3$  happen not be Galois subcovers of  $\mathcal{H}_{27}$ . A partial list of them is given in the following proposition.

**Corollary 5.2.** *The quotient curves  $\mathcal{R}_3/G_1$ ,  $\mathcal{R}_3/G_2$ , and  $\mathcal{R}_3/G_3$  are not Galois subcovers of  $\mathcal{H}_{27}$  for the groups  $G_1, G_2, G_3$  defined as follows.*

- *The maximal subgroups  $G_1 \leq \text{Ree}(3)$  of order 24 centralizing an involution  $\sigma \in \text{Ree}(3)$ , which are isomorphic to  $\langle \sigma \rangle \times \text{Alt}(4)$ .*
- *The groups  $G_2 \leq \text{Ree}(3)$  of order 6 which are isomorphic to  $\text{Sym}(3)$ .*
- *The cyclic groups  $G_3 \leq \text{Ree}(3)$  of order 6.*

*Proof.* From previous work of Çakçak and Özbudak, each of the quotient curves  $\mathcal{R}_3/G_1$ ,  $\mathcal{R}_3/G_2$ , and  $\mathcal{R}_3/G_3$  has genus 2; see [2, Sec. 4.1.1, p. 150] for  $\mathcal{R}_3/G_1$ , [2, Sec. 4.2, pp. 163-164] for  $\mathcal{R}_3/G_2$ , and [2, Sec. 4.4, pp. 171] for  $\mathcal{R}_3/G_3$ . On the other hand, Theorem 5.1 shows that no  $\mathbb{F}_{27^2}$ -maximal curve of genus 2 is a Galois subcover of  $\mathcal{H}_{27}$ .  $\square$

## 6. ACKNOWLEDGEMENTS

This research was supported by the Italian Ministry MIUR, Strutture Geometriche, Combinatoria e loro Applicazioni, PRIN 2012 prot. 2012XZE22K, and by GNSAGA of the Italian INdAM.

## REFERENCES

- [1] Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. *J. Symbolic Comput.* **24** (3-4), 235–265 (1997).
- [2] Çakçak, E., Özbudak, F.: Subfields of the function field of the Deligne-Lusztig curve of Ree type. *Acta Arith.* **115**, 133–180 (2004).
- [3] Çakçak, E., Özbudak, F.: Number of rational places of subfields of the function field of the Deligne-Lusztig curve of Ree type. *Acta Arith.* **120**, 79–106 (2005).
- [4] Cossidente, A., Korchmáros, G., Torres, F.: On curves covered by the Hermitian curve. *J. Algebra* **216**, 56–76 (1999).
- [5] Cossidente, A., Korchmáros, G., Torres, F.: Curves of large genus covered by the Hermitian curve. *Comm. Algebra* **28**, 4707–4728 (2000).
- [6] Deligne, P., Lusztig, G.: Representations of reductive groups over finite fields. *Ann. of Math.* **103**, 103–161 (1976).
- [7] Duursma, I., Mak, K.: On maximal curves which are not Galois subcovers of the Hermitian curve. *Bull. Braz. Math. Soc. (N.S.)* **43** (3), 453–465 (2012).
- [8] Fuhrmann, R., Torres, F.: On Weierstrass points and optimal curves. *Rend. Circ. Mat. Palermo Suppl.* 51 (Recent Progress in Geometry, Ballico E, Korchmáros G, (Eds.)), 25–46 (1998).
- [9] Garcia, A.: Curves over finite fields attaining the Hasse-Weil upper bound. In: *European Congress of Mathematics*, vol. II (Barcelona 2000), Progr. Math. 202, pp. 199–205. Birkhäuser, Basel (2001).
- [10] Garcia, A.: On curves with many rational points over finite fields. In: *Finite Fields with Applications to Coding Theory, Cryptography and Related Areas*, pp. 152–163. Springer, Berlin (2002).

- [11] Garcia, A., Güneri, C., Stichtenoth, H.: A generalization of the Giulietti-Korchmáros maximal curve. *Adv. Geom.* **10** (3), 427–434 (2010).
- [12] Garcia, A., Stichtenoth, H.: Algebraic function fields over finite fields with many rational places. *IEEE Trans. Inform. Theory* **41**, 1548–1563 (1995).
- [13] Garcia, A., Stichtenoth, H.: A maximal curve which is not a Galois subcover of the Hermitian curve. *Bull. Braz. Math. Soc. (N.S.)* **37**, 139–152 (2006).
- [14] Garcia, A., Stichtenoth, H., Xing, C.P.: On subfields of the Hermitian function field. *Compositio Math.* **120**, 137–170 (2000).
- [15] Giulietti, M., Hirschfeld, J.W.P., Korchmáros, G., Torres, F.: A family of curves covered by the Hermitian curve. *Sémin. Congr.* **21**, 63–78 (2010).
- [16] Giulietti, M., Korchmáros, G.: A new family of maximal curves. *Math. Ann.* **343** (1), 229–245 (2009).
- [17] Giulietti, M., Korchmáros, G., Torres, F.: Quotient curves of the Deligne-Lusztig curve of Suzuki type. *Acta Arith.* **122**, 245–274 (2006).
- [18] Giulietti, M., Montanucci, M., Zini, G.: On maximal curves that are not quotients of the Hermitian curve. arXiv:1511.05353.
- [19] Giulietti, M., Quoos, L., Zini, G.: Maximal curves from subcovers of the GK-curve. *J. Pure Appl. Algebra*, to appear.
- [20] Hansen, J.P.: Deligne-Lusztig varieties and group codes. In: *Coding Theory and Algebraic Geometry, Lecture Notes in Mathematics*, vol. 1518, pp. 63–81. Springer, Berlin (1992).
- [21] Hansen, J.P., Pedersen, J.P.: Automorphism groups of Ree type, Deligne-Lusztig curves and function fields. *J. Reine Angew. Math.* **440**, 99–109 (1993).
- [22] Hartley, R.W.: Determination of the ternary collineation groups whose coefficients lie in the  $GF(2^n)$ . *Ann. of Math. Second Series* **27** (2), 140–158 (1925).
- [23] Hirschfeld, J.W.P., Korchmáros, G., Torres, F.: *Algebraic Curves over a Finite Field*. Princeton Series in Applied Mathematics, Princeton (2008).
- [24] Hoffer, A.R.: On unitary collineation groups. *J. Algebra* **22**, 211–218 (1972).
- [25] Hughes, D.R., Piper, F.C.: *Projective Planes*. Graduate Text in Mathematics **6**, Springer, Berlin (1973).
- [26] Hurt, N.E.: *Many Rational Points: Coding Theory and Algebraic Geometry*. Mathematics and Its Applications **564**, Springer, Berlin (2003).
- [27] Kantor, W.N., O’Nan, M.E., Seitz, G.M.: 2-Transitive Groups in Which the Stabilizer of Two Points is Cyclic. *J. Algebra* **21**, 17–50 (1972).
- [28] Lachaud, G.: Sommes d’Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis. *C.R. Acad. Sci. Paris* 305, Série I, 729–732 (1987).
- [29] Mak, K.H.: On Congruence Function Fields with many rational places. PhD Thesis, [www.ideals.illinois.edu/bitstream/handle/2142/34193/Mak\\_KitHo.pdf?sequence=1](http://www.ideals.illinois.edu/bitstream/handle/2142/34193/Mak_KitHo.pdf?sequence=1).
- [30] Mitchell, H.H.: Determination of the ordinary and modular ternary linear groups. *Trans. Amer. Math. Soc.* **12** (2), 207–242 (1911).
- [31] Neumann, P.M., Stoy, G.A., Thompson, E.C.: *Groups and Geometry*. Oxford University Press, Oxford (1994).
- [32] Pasticci, F.: On quotient curves of the Suzuki curve. *Ars Combin.* **97A**, 429–446 (2010).
- [33] Pedersen, J.P.: A function field related to the Ree group. In: *Coding Theory and Algebraic Geometry, Lectures Notes in Mathematics*, vol. 1518, pp. 122–132. Springer, Berlin (1992).
- [34] Rose H.E.: *A Course on Finite Groups*. Springer Science and Business Media, London (2009).
- [35] Singh, S., Zameeruddin, Q.: *Modern Algebra*, 8th edn. Vikas Publishing House, New Delhi (2006).
- [36] Monakhov, V.S.: Normal subgroups of biprimary groups. *Mat. Zametki* **18** (6), 877–886 (1975).

- [37] Stichtenoth, H.: *Algebraic function fields and codes*, 2nd edn. Graduate Texts in Mathematics **254**. Springer, Berlin (2009).
- [38] Tafazolian, S., Teherán-Herrera, A., Torres, F.: Further examples of maximal curves which cannot be covered by the Hermitian curve. *J. Pure Appl. Algebra* **220** (3), 1122–1132 (2016).
- [39] Tate, J.: Endomorphisms of abelian varieties over finite fields. *Invent. Math.* **2**, 134–144 (1966).
- [40] van der Geer, G.: Curves over finite fields and codes. In: *European Congress of Mathematics*, vol. II (Barcelona 2000), Progr. Math. 202, pp. 225–238. Birkhäuser, Basel (2001).
- [41] van der Geer, G.: Coding theory and algebraic curves over finite fields: a survey and questions. In: *Applications of Algebraic Geometry to Coding Theory, Physics and Computation, NATO Sci. Ser. II Math. Phys. Chem.* 36, pp. 139–159. Kluwer, Dordrecht (2001).